

REMARKS

Introduction

Claims 1-3, 5-12, 14-24, 26-33, 35-44 and 46 are currently pending in the present application. Claims 4, 13, 25, 34 and 45 and 47-55 are cancelled. For at least the reasons set forth below, Applicants submit the claims are in condition for allowance.

Amendment of Claims

Claims 1, 22 and 43 are amended to include recitation of elements previously found in claims 13 and 34 respectively, and therefore do not add any new matter. Claim 3 is amended to reflect the amended lettering of amended claim 1. Claims 13 and 34 are accordingly cancelled, without prejudice. Claims 4, 25, 45 and 47-52 are cancelled based upon withdrawal from consideration. Claims 53-55 are also cancelled, without prejudice.

Rejection of claims under 35 U.S.C. §102(e)

Claims 1-3, 5-24, 26-44, 46 and 53-55 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,530,024 (hereinafter referred to as "Proctor"). As to claims 1-3, 5-12, 14-24, 26-33, 35-44 and 46, the rejection is improper because Proctor fails to identically disclose each of the claimed limitations.

To anticipate a claim under 35 U.S.C. §102(e), a single prior art reference must identically disclose each and every claim feature. See Lindeman Maschinenfabrik v. American Hoist and Derrick, 730 F.2d 1452, 1458 (Fed. Cir. 1984). If any claim feature is absent from a prior art reference, it cannot anticipate the claim. See Rowe v. Dror, 112 F.3d 473, 478 (Fed. Cir. 1997).

Claims 1, 22 and 43 are directed to monitoring events generated on a computer system including various steps, for example monitoring a set of event data, recording the event data in a database, interrogating the database and reading alert event data if an action is determined to violate one of the predefined rules. Claims 1, 22 and 43, as amended, further include the limitation previous recited in claims 13 and 34, specifically "determining said action response based upon said pre-defined set of rules and based upon a weighting factor applied to recorded historical outcomes for monitored events." as recited in amended claim 1. Therefore, in addition to monitoring current events, the claimed invention also includes the weighting factor that is applied to "recorded historical outcomes for monitored events." As illustrated in Fig.7, steps S710-S770 and page 13, line 20 to page 14, line 15 of the Application, the approach can be used to look at previous events to determine if one or more

events have any historical significance. This technique can determine, for example, if an event may have been apart of a long term attack, for example.

Proctor is directed to a security system and methods of adapting security procedures based on computing environment activity, the methods including the creating an implementation of one or more security procedures. As understood, Proctor discloses an adaptive feedback system that actively monitors the processing environment and detects security incidents based on implemented security procedures. In its adaptive feedback system, Proctor allows security policies to actively updated. For example, in the Proctor system security procedures are applied to target computers 104A. In response to a collection policy, the system logs target computer activities. The security console 104B monitors these logged elements in response to the audit policy. Additionally, the agents 112 (either on the target computers 104A or the security console 104B) review the log files to determine if any security breaches have occurred. (See, for example, col. 6, lines 53-65). If any breaches have occurred, Proctor provides for an appropriate security response, such as illustrated in step 224 of Fig. 2.

Proctor's adaptive system also teaches adjusting the security levels on a going-forward basis based on the detection security breach. Col. 7, lines 15-41 disclose several embodiments including adjusting a security policy, such as to either "tightened" or "relaxed." Therefore, the Proctor system can adjust the scrutiny level of one or more user based on detected events.

The method of Procter includes an audit policy to define or identify activities in the computing environment to be audited and can include logging of the audited events. Procter teaches that audit policies are generally known (col. 6 line 8 to 11) and define the activities to look for in the computing environment. To establish the audit policy, Procter requires that a network administrator identify to the security system the types of events and actions that it should monitor, that is, specific policies are identified to the system and the system then monitors and possibly logs events that fall within the particular audit policy (see for example col. 6, lines 21 to 38). The security system of Proctor only identifies and logs those events that satisfy the deterministic audit policy settings – events that are not defined in the audit policies are not captured and not logged to compare against future events or amended (or new) audit policies.

This is an undesirable situation since the security system of Proctor can not identify events that may possibly be malicious if the event type is previously unknown – such as in the case of a new virus that is programmed to take advantage of a newly discovered security

defect in a particular software application. For the security system of Proctor to be able to identify such malicious attacks, the vulnerability must be first identified in the software application and a new audit policy to be defined such that the system can react to the attack if it occurs. This is a deterministic approach that is often unable to be implemented effectively. The range of new vulnerabilities being exposed and taken advantage of typically occurs on a much faster time scale than the identification and categorization of such attacks. Therefore, the dissemination of the required knowledge to network administrators to enable a suitable audit policy prior to a malicious attack event is generally delayed. Accordingly, it is often the case that an attack event has already occurred by the time a suitable audit policy to monitor for that particular type of attack has been implemented in the security system.

More importantly, in the security system of Proctor, the event logs that do not have a corresponding audit policy policing for that particular type of event are deleted to reduce the amount of logged events that a network administrator must analyze. Accordingly, if a new type of malicious attack is identified, it is impossible to check the recorded logs for instances of that type of attack and identify whether the network environment has already been compromised.

In contrast, the present invention, as described in the present application, utilizes not only predefined policies that watch for known events within the networked environment, but also uses historical data to analyze each current event log and compare it against the historical event logs. In this way the present invention is able to distinguish those events that are abnormal from the typical events seen in the monitored environment. This use of historical data to determine whether a particular event is historically significant is described in the specification on page 14 lines 8 to 15 and the method described in further details on page 17 lines 18 to 28 with reference to Figure 8.

In the applicant's invention, the event data is derived from a data feed from the Application Agent Modules (AAMs) and System Agent Modules (SAMs) which act merely as data collectors for the present invention. The data feed is not restricted to data from logfiles or network traffic information, but rather the event data that is recorded and subsequently used in the current system can be derived from any data feed of interest. For example, event data sources can include the network transport layer, the security layer, or data from third party or proprietary application programs (page 8, lines 19 to 21).

Relevant event data is extracted from the data feed, placed in a universal format and assigned an event code (page 12, lines 13 to 24). All this extracted event data is then recorded in the database 318. In this way, the inference engine can examine all the historical

event data for anomalies compared with the “normal” traffic when it encounters an event for which no specific response trigger currently exists.

In contrast, in the system of Proctor, only event data that has already triggered a response from the system in line with the already existing audit policies that have been configured in the system are collected (see col. 11 lines 30 to 33, col. 14 lines 26 to 27). Proctor primarily operates in this manner to enable the amount of audit records to be reduced into a usable quantity by eliminating unnecessary data. This process, however, effectively destroys the integrity of the security records since the entire event data history cannot be re-examined to determine if a security incident has previously occurred that did not fall under the initial audit policies – the records are irretrievably lost and security audit capabilities severely limited.

Claims 1, 22 and 43, as amended, recites determining said action response “based upon said pre-defined set of rules and **based upon a weighting factor applied to recorded historical outcomes for monitored events.**” (emphasis added). Proctor fails to identically disclose, among other things, determining its alert response based upon a weighting factor applied to recorded historical outcomes for monitored events. In support of the original rejection of claims 13 and 34, the Examiner cites to the above-noted passage of Col. 7, lines 15-41, to which Applicants respectfully disagree. The Examiner-noted passage discloses adjusting the monitoring level, but this adjustment (for example to a “tightened” setting) is not disclosed as being based upon a weighting factor applied to recorded historical outcomes for monitored events. Even assuming the Examiner asserts the weight factor as being the adjusted monitoring level, this weight factor is not applied to “recorded historical outcomes for monitored events.” Rather, as expressly disclosed in Proctor, when the monitoring level is adjusted, it is adjusted to look for future events. The advantage that the applicant’s invention has over the system of Proctor is that anomalous behavior or events in the data feed can be detected long before a specific rule can be configured for that type of event.

Therefore, Proctor lacks the ability to detect if an event has previously occurred without being detected, such as a determining if any activity is a long term security attack. Proctor fails to identically disclose claims 1, 22 and 43 because Proctor fails to disclose, among other things, applying a weighting factor to previously logged activities.

As to claims 2-3, 5-12, 14-22,, 23, 26-33, 35-42, 44 and 46, these claims depend from claims 1, 22 and 43, respectively, and recite further patentable subject matter in view thereof. For at the least reasons stated above with respect to claims 1, 22 and 43, Proctor further fails

to identically disclose the limitations of dependent claims 2-3, 5-12, 14-22,, 23, 26-33, 35-42, 44 and 46.

As to claims 13, 34 and 53-55, the rejection is moot in view of the cancellation of these claims.

Therefore, Applicants submit the rejection is improper and claims 1-3, 5-12, 14-24, 26-33, 35-44 and 46 are patentable in view of Proctor. Applicants respectfully request reconsideration and withdrawal of this rejection.

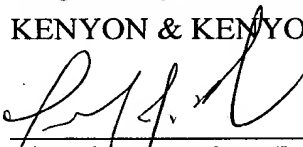
Conclusion

In light of the foregoing, Applicants respectfully submit that all of the pending claims are in condition for allowance. It is therefore respectfully requested that the rejections be withdrawn. Prompt reconsideration and allowance of the present application are therefore respectfully requested.

Respectfully submitted,
KENYON & KENYON

Dated: February 21, 2006

By:



Timothy J. Bechen (Reg. No. 48,126)
One Broadway
New York, New York 10004
(212) 425-7200

CUSTOMER NO. 26646

26646

26646

PATENT TRADEMARK OFFICE